27. The method of claim **16**, wherein the at least one operating point is ascertained by ascertaining an intended operating range on a basis of a configuration of the automation installation.

28. The method of claim **27**, wherein the at least one possible operating point is ascertained by taking into consideration only extreme values for manipulated variable restrictions of installation components.

29. An engineering system for designing and/or configuring an automation installation having at least two control apparatuses for controlling a controlled system, said engineering system comprising an analysis device configured to take a present topology model of the automation installation and a process model of a process to be performed via the automation installation as a basis for ascertaining the resultant controlled system and a down time caused by a changeover between the control apparatuses, said analysis device configured to:

provide a controlled system and at least two control apparatuses, said at least two control apparatus alternately controlling the controlled system during a normal operation by outputting control outputs, said automation installation operating a process via the control system;

prompt a changeover between the at least two apparatuses at a failure;

continuously operate the controlled system during the changeover in a controller-less operation for a down time;

ascertain a possible operating point for the controlled system during the normal operation;

simulate a controller-less operation for each operating point for a duration of the down time to thereby ascertain a state trajectory starting out from the operating point for the controlled system;

check whether the state trajectory fails to meet a predetermined safety criterion; and if affirmative

initiate a predetermined protective measure to avoid the at least operating point.

30. An automation installation having a controlled system for operating a process and having at least two control apparatuses for failsafe and alternate control of the controlled system, said automation installation being configured to monitor a failure tolerance during operation by:

providing a controlled system and at least two control apparatuses, said at least two control apparatus alternately controlling the controlled system during a normal operation by outputting control outputs, said automation installation operating a process via the control system;

prompting a changeover between the at least two apparatuses at a failure;

continuously operating the controlled system during the changeover in a controller-less operation for a down time;

ascertaining a possible operating point for the controlled system during the normal operation;

simulating a controller-less operation for each operating point for a duration of the down time to thereby ascertain a state trajectory starting out from the operating point for the controlled system;

checking whether the state trajectory fails to meet a predetermined safety criterion; and if affirmative

initiating a predetermined protective measure to avoid the at least operating point.

* * * * *